Network Requirements

Firewall rules and network configuration guide

1. Overview

SummitView requires only outbound HTTPS (port 443) connections. No inbound firewall rules or port openings are required. This document provides the complete list of network destinations that must be reachable from the machine running the SummitView Agent or Cloud Connect.

2. Key Points

- All connections are outbound HTTPS (TCP port 443) only
- No inbound firewall rules required
- No VPN or site-to-site connection needed
- No reverse connections — the agent initiates all traffic
- Compatible with corporate proxy servers (HTTP/SOCKS)

3. Required Outbound Connections

Direction	Protocol	Destination	Port	Purpose
Outbound	HTTPS	summitview.app	443	SummitView cloud API
Outbound	HTTPS	*.analysis.windows.net	443	Power BI REST APIs
Outbound	HTTPS	login.microsoftonline.com	443	Azure AD authentication
Outbound	HTTPS	graph.microsoft.com	443	Microsoft Graph (optional)
Outbound	HTTPS	*.pbidedicated.windows.net	443	XMLA endpoints (PPU/Fabric)
Inbound	None	N/A	N/A	No inbound connections

4. Endpoint Details

summitview.app

- Agent registration and heartbeat
- Metrics data transmission (refresh times, inventory, usage events)
- Hosted on Vercel CDN (global edge network)

***.analysis.windows.net**

- Power BI REST API calls for workspace, dataset, report, and refresh data

- Read-only API access (Dataset.Read.All, Workspace.Read.All, Report.Read.All)
- Includes api.powerbi.com which resolves to this domain

login.microsoftonline.com

- Azure AD OAuth 2.0 token acquisition and refresh
- Required for agent authentication

graph.microsoft.com (optional)

- Used for user profile information during SSO
- Not required for core agent functionality

***.pbidedicated.windows.net (PPU/Fabric only)**

- XMLA endpoint for per-table refresh timing
- Only used with Premium Per User (PPU) or Fabric workspaces
- Not required for Pro-only environments

5. Proxy Configuration

If your environment requires a proxy server for outbound HTTPS traffic:

- The agent respects system-level proxy settings configured in Windows
- HTTP and SOCKS proxy types are supported via .NET system proxy
- SSL inspection proxies: ensure the proxy CA certificate is in the Windows certificate store
- If using proxy authentication, configure credentials in the Windows proxy settings

6. Bandwidth Requirements

SummitView agent traffic is minimal:

- Heartbeat: ~1 KB every 30 seconds
- Refresh sync: ~5-50 KB per sync cycle (depends on number of datasets)
- Inventory sync: ~10-100 KB per sync (depends on workspace count)
- Usage sync: ~5-200 KB per sync (depends on activity volume)
- Total estimated: < 10 MB per day for a typical environment

7. Troubleshooting Connectivity

If the agent cannot reach SummitView cloud:

- Verify outbound HTTPS (443) is allowed to summitview.app

- Check proxy settings if applicable
- Test connectivity: curl https://summitview.app/api/health
- Review Windows Event Log for agent error messages
- Contact security@summitview.app for assistance